



Australian Government
Department of Defence
Estate and Infrastructure Group

Department of Defence
Estate and Infrastructure Group

**BASE SERVICES CONTRACT OPERATING INSTRUCTION
FOR OBJECTIVE AND DEFENCE INFORMATION
MANAGEMENT**



October 2015

Authorisation

The Base Service Contract Operating Instruction to Objective and Defence Information Management will be released under the authority of the undersigned.

Gary Todd
Director Data and Information Governance
Estate and Infrastructure Group

October 2015

Document review and Approval

Revision History

Version	Author	Date	Revision
0.9	DSO Data and Information Governance	May 2015	Reviewed
1.0	DSO Data and Information Governance	Aug 2015	First version
2.0	ESD Data and Information Governance	Sep 2015	Second version <small>*Note: Defence Support Operations has changed to Estate Services Division. Objective naming of Workgroups and folders still uses DSO until otherwise advised/updated.</small>
3.0 & 4.0	Data and Information Governance	Oct 2015	Third and Fourth Version

This document has been approved by

Name	Signature	Date reviewed
DDIG Gary Todd		Oct 15

Amendment

Proposals for amendment to the Objective Instruction must be forwarded to the Director Data and Information Governance (DDIG).

Table of Contents

TABLE OF CONTENTS	III
SECTION 1 – INTRODUCTION	5
Purpose	5
Priority of this Instruction	5
Scope of this Instruction.....	5
Definitions	5
Background.....	6
Benefits of Using Objective	6
Security Classification of Documents	7
Key Stakeholders	8
Folder Structure Overview	9
SECTION 2 - GETTING STARTED	11
Overview	11
Key Roles and Responsibilities.....	11
Directorate Data and Information Governance	11
Defence National Work Group Coordinators	11
Defence Work Group Coordinators.....	12
Product & Service Managers (Defence Sponsors).....	12
Contractor Work Group Coordinators.....	12
Contractor Sponsor	13
Contractor Objective User.....	13
Getting access to the Defence Restricted Network and Objective	13
SECTION 3 – DIGITAL RECORDKEEPING AND INFORMATION & SYSTEM SECURITY	16
Digital Recordkeeping	16
Information and System Security Requirements	16
User Groups (Workgroup Groups) and Work Group Coordinator Groups.....	17
Privileges	17
SECTION 4 – DEIS BUSINESS RULES	19
Acceptable File Types.....	20
Business Rules	20
Document Scanning	21
Imagery	21
Uploading Documents to Objective and Digital Storage Devices	21
Filing Documents in Objective.....	21
General Uploads to Objective	22

Defence Email.....	22
External File Servers Downloads	22
CD and DVDs	22
Portable Electronic Devices – USB read-only multi-card reader	22
USB Sticks and Portable Hard Drives.....	23
Objective to IBIS	24
Documents / Records Generated Under Base Services Contracts	24
File Naming Convention	24
Metadata requirements for records in Objective	25
SECTION 5 - SYSTEM SUPPORT – USEFUL LINKS	26
Annex A - Estate Management Folders, Intended Use, Ownership and Key Stakeholders	27
Annex B – Defence National Work Group Coordinators	28
Annex C - Estate Management Folder Structure.....	29
Annex D – Estate Management Folders, Main User Groups.....	30
Annex E – Estate Management Folders, Folder Owners and Purpose of Folder Area.....	31
Annex F – Estate Management Folders (1 – 7) – Folder Hierarchy	32
Annex G – Flowchart: Contractor Access to Objective– Estate Management Folders	33
Annex H – Product and Service Line Matrix – Contract Authorities, Contractors and PSMs	34
Annex I – CAMPUS Screenshot showing Objective courses.....	35
Annex J – Objective User Account Access Request via ICT Service Portal (Post CAMPUS Training).....	36
Annex K – Objective Contractor Access Request Form to Estate Management Folders	37
Annex L – Minimum Scanning Specifications (Extract from RECMAN).....	38
Annex M – Document Descriptors, File Placement, Key Stakeholders and Estimated Document Size.....	39
Annex N – Objective Metadata Requirements – Extract of Catalogue (Draft).....	43
Acronyms.....	45

Section 1 – Introduction

Purpose

- 1.0 The purpose of this document is to provide the governance and operating instructions to the Estate Maintenance and Operations Services (EMOS) contractors , Miscellaneous Services Package (MSP) contractors and Estate Services Division (ESD) personnel for the lodgement, classification, maintenance and storage of estate management and contract related information. Adherence with this operating instruction will assist with consistent, compliant and efficient management of information.
- 2.0 Objective, Defence's mandatory records and document management system, forms part of the Defence Estate Information Systems (DEIS).

Priority of this Instruction

- 3.0 Ambiguity, inconsistency or discrepancy between this instruction and any of the Base Services Contracts and Commonwealth or Defence issued policy, will be interpreted in the following order of priority to the extent of any ambiguity, inconsistency or discrepancy:
 - 3.1 Commonwealth Legislation;
 - 3.2 Base Services Contracts;
 - 3.3 Defence Policy; and
 - 3.4 this Operating Instruction.

Scope of this Instruction

- 4.0 This Operating Instruction covers:
 - 4.1 the operating policy and use of Objective;
 - 4.2 the purpose and structure of the Estate Management folder;
 - 4.3 the use of the Estate Management sub-folders including uploading of Estate related documentation to IBIS;
 - 4.4 the Objective users' roles and responsibilities and system support;
 - 4.5 the document types typically required to be stored in Objective under the Base Services Contracts; and
 - 4.6 file and document formats, specifications and naming conventions.
- 5.0 Documents required to be stored in the National Spatial Information Management System (NSIMS) is subject to a separate Operating Instruction for NSIMS.

Definitions

- 6.0 A Corporate file consists of a collection of documents, emails and objects that record an organisation's business and policy decisions. A Corporate file can be one of the following within Objective: Virtual, Physical and Mixed mode. Virtual files are created in and managed by Objective, but have no physical equivalent, and contain only electronic documents. Physical files are created and handled physically, recorded in and managed by Objective. Mixed mode files contain both Virtual and Physical

documents. Note that new physical files should not be created in the EM folder structure as files are expected to be supplied electronically.

- 7.0 Document is defined as an artefact that possesses information. It can be one or more of the following; word document, portable document format (PDF), spreadsheet, drawing, chart, map, image, scan, brochure, manual, certificate or any other item that is not broken down into a data string for inclusion into a database.
- 8.0 Data can be defined as the representation of raw, unorganised facts that need to be captured, stored or processed. Data can be something simple and seemingly random and useless until it is organised. IBIS and GEMS are the key data systems that EMOS and MSP contractors will interact with. The bulk of the data provided by the EMOS and MSP contractors to IBIS and GEMS will reflect changes made to the Defence Estate. These changes are referred to as modified Estate Master Data or more commonly referred to as Estate Records.
- 9.0 Defence Record. A Defence record is any document or object, in any form, that contains information relating to Defence activity, and is created, captured, managed or stored by any Defence personnel or external service provider in order to provide evidence of that activity.

Background

- 10.0 Objective is Defence's record management system mandated by the Defence Committee in November 2009. The system operates on both the Defence Secret and Restricted Networks and enables electronic documents to be managed through their entire life cycle, from creation through to review and once finished with, archival or disposal.
- 11.0 The National Archives of Australia has developed a Digital Continuity Policy for whole of government which requires all Commonwealth entities to move to a digital information and records management system by the target date of 2020. Digital Continuity targets for 2020 have been set by the Archives Minister and may be found at this web location: www.naa.gov.au.
- 12.0 Information provided by Contractors under the former sub-regional contract model has been managed in an ad hoc and decentralised manner. Former document management arrangements were complicated by the fact that each Defence region had adopted different information management practices. This resulted in inconsistent processes for the storage, classification and retention of soft copy documents.

Benefits of Using Objective

- 13.0 EMOS and MSP Contractors are required to register all Defence records generated and/or associated with the Defence Estate and required under their contract in Objective. These documents may be generated by the Contractor or their subcontractors or collected on behalf of Defence from another Contractor.
- 14.0 Contractors and ESD personnel utilising the Objective system in the prescribed way will eliminate many of the issues about the promulgation of information relating to the Defence Estate.
- 15.0 The registration of documents in Objective provides a number of benefits in supporting contractual activities. Documents uploaded into Objective will provide greater transparency of information to all stakeholders in a timely and secure way as well as providing a detailed audit of activity for each object registered. In addition, registration in Objective will:
 - 15.1 form part of the 'evidence' that supports adherence to Commonwealth, State and local legislation, Defence and Commonwealth policy and contractual compliance associated with the Defence Estate;

- 15.2 support the sharing of intelligence between Contractors and Defence about the Defence Estate including its condition, risks, and maintenance;
- 15.3 inform decisions about the Defence Estate and contract obligations;
- 15.4 ensure Defence records relating to service delivery and contractual obligations are captured within a secure yet selectively transparent environment;
- 15.5 form part of the evidentiary trail that a contractor and/or Defence activity was performed; and
- 15.6 provide a central records storage facility in which documents can be retrieved, edited, reproduced, preserved, approved and archived.

Security Classification of Documents

- 16.0 Documents stored in Objective have to be classified as either UNCLASSIFIED or For Official Use Only (FOUO). Documents classified as Protected must be stored in accordance with the relevant Defence Product and Service Manager (PSM) direction. All other classifications (SECRET/TOP SECRET) are not part of this instruction and documents classified higher than Protected must not be stored in Objective on the DRN.

Table 1: List of Defence Security Classifications for Documents

Document Classification	Definition	Instruction
UNOFFICIAL	The marking UNOFFICIAL may be assigned to information that people generate in their private capacity under reasonable use of Defence resource provisions.	This classification is NOT to be used. All documents stored in Objective must be as a result of official business and/or contract activities.
UNCLASSIFIED	Official information that does not meet the criteria for the application of a security classification (see paragraph 30.45) of the Defence Security Manual (DSM) is UNCLASSIFIED official information.	This classification can be used to store documents in Objective as long as it meets the classification criteria.

Document Classification	Definition	Instruction
FOR OFFICIAL USE ONLY (FOUO)	Official information that meets the criteria for FOUO.	<p>This classification can be used as long as it meets the classification criteria.</p> <p>FOUO documents can only be added to Objective via a DRN account.</p> <p>PSMs should be issued any additional handling instructions.</p>
PROTECTED	Official information that meets the criteria set out for Protected.	<p>This classification can be used as long as it meets the classification criteria.</p> <p>Protected documents can only be added to Objective via a DRN account.</p> <p>Where a requirement for a document to be classified as Protected, the PSM should be notified of the intention to upload the document and any additional document handling instructions required before the document is uploaded to Objective.</p>
SECRET	Not to be used in this instruction.	Document with this classification must not be stored in Objective via the DRN.
TOP SECRET	Not to be used in this instruction.	Document with this classification must not be stored in Objective via the DRN.

Key Stakeholders

17.0 The Estate Management folder is set up in Objective so that stakeholders can create, register, store and locate documents relating to the Defence Estate, a Base Services contract deliverable or an estate development, investment, leasing, disposal or maintenance project. Key stakeholder groups include:

17.1 EMOS Contractors;

17.2 other Base Services Contractors;

- 17.3 Infrastructure Division Contractors; and
- 17.4 Estate Services Division Personnel.
- 18.0 Annex A provides a breakdown of stakeholders for the respective folders within the Estate Management area, including folder ownership and the nominated WGC.
- 19.0 A National Workgroup Coordinator group has been established to oversee the Estate Management (EM) Work Group in terms of Objective issues, structural and process changes. A list of members and their contact details are set out in Annex B.

Folder Structure Overview

- 20.0 The EM Work Group and subordinate folders within Objective provides a centralised storage facility for documents relating to and associated with the Defence Estate and Base Services Contracts.
- 21.0 The folder structure within the EM Work Group provides four main areas which are outlined below and explained in Annex E.
- 22.0 **Estate Management:** Under each folder (1-7), a “corporate file” is created for each Defence property. The EM folders (refer annex F), under the EM Work Group contain a corporate file for every Defence property regardless of whether it is owned, leased or subject to disposal. Each part of the Defence Estate is categorised according to its estate classification (refer Section 4 - DEIS Business Rules for further information). Under folder “02 Defence Support – National”, each Base Services product and service has a folder to be used for their business purposes, as agreed with the individual PSM.
- 23.0 Documentation relating to a property must be stored in the correct folder under that property. DDIG are responsible for creating new folders in the EM folder structure to reflect changes made to the Defence Estate and the associated estate records held in IBIS.
- 24.0 **A Base Services Contractor - DEPOSIT BOXES:** Each Base Services Contractor has a Deposit Box folder created for their use. These folders allow the Contractor, Product and Service Managers (PSMs), Contract Authorities (CAs) and any other Defence stakeholders to access the same information concurrently. It provides a staging area for documents so that stakeholders may quickly and easily view and perform necessary activities pertaining to that information.
- 25.0 The use of the Contractor Deposit Box areas will be largely determined by business needs and that which is arranged between the various stakeholders. Contractors may set-up folders and subfolders within their Deposit Boxes to suit business needs, however, it is strongly recommended that the Product and Service line folders are maintained as a minimum. Refer to Annex D.
- 26.0 **B Contract Administration Support – Contract Change Proposals:** These folders will ultimately be available for use by each Base Services Contractor to upload Contract Change Proposals, edit information and track progress. Approved contract change proposals may be downloaded from this area.
- 27.0 **C Defence Fuel Installation (DFI) Documentation:** This folder currently stores some DFI documentation that is undergoing a migration activity to place these records within their respective Property File in the relevant Estate Management folders 03 – 07. Once this activity has been completed, the DFI folder structure will be removed.
- 28.0 **D Estate and Facilities Services Project Documentation:** This folder area provides a centralised storage area for historical project documentation traditionally kept by Estate and Facility Services. The folder is temporary until it is determined whether or not the information needs to be transferred to the EM folders. Contractors who require access to this information may access it upon request (refer to Annex A for WGC).

- 29.0 Other folders within the EM area may be created and removed as business needs require. For the creation or removal of folders under the EM area, contact DDIG or a National Work Group Coordinator.

Section 2 - Getting Started

Overview

- 30.0 To access Objective, the minimum access requirements for users are:
 - 30.1 a Baseline security clearance or higher;
 - 30.2 a Defence Restricted Network (DRN) account; and
 - 30.3 successful completion of the relevant CAMPUS online courses (see below).
- 31.0 Annex G provides a flowchart of the overall access process – it does not detail the sub-processes as they are already established and instruction may be found on the Defence intranet.
- 32.0 Each Contractor must nominate a minimum of two WGCs. Users designated as a WGC must complete the Work Group Coordinator training found on CAMPUS online. The role of WGC is to provide assistance to their designated Objective users and is further defined under the Key Roles and Responsibilities under this section. It is not intended that Contractor WGCs (CWGCs) have access to internal Product and Service directorate management information, which is stored in the DSO work group rather than the Estate Management workgroup.

Key Roles and Responsibilities

- 33.0 All Objective users have a responsibility to abide by Defence Information Management policies. In doing so, they are accountable for the appropriate handling of the records for which they are responsible.
- 34.0 The file structure in a Work Group is constructed and managed by the designated WGC, and should be designed around an effective structure for that business area. Defence has already created many of the sub-folders in the Estate Management Work Group and has assigned Defence WGCs to help manage the folder areas.
- 35.0 The following roles provide an outline of key responsibilities for Contractors and Defence in managing Defence records within the Estate Management Work Group of Objective.

Directorate Data and Information Governance

- 36.0 Data & Information Governance oversees the implementation of structures, policies, procedures, processes, data and controls to manage information and maintain quality and controls over data, in line with ESD requirements. In particular, DDIG provides the operating guidance for the use of ESD's Objective system, folder structure, storage and naming of documentation including the metadata stored with each document.

Defence National Work Group Coordinators

- 37.0 Made up of Principle and Work Group Coordinators, the Defence National Work Group Coordinator (NWGC) group has evolved as a result of change in ESD's Operating Model. A list of Defence NWGC and their contact details is in Annex B.
- 38.0 NWGCs assist DDIG to ensure ESD's information management standards are maintained. They are the liaison between DDIG, Objective Administration and other WGCs (Defence and Contractor).
- 39.0 NWGCs have a default access to all ESD Work Groups within Objective and facilitate Contractor Access to respective folders within the Estate Management area. NWGCs assist with the overall structure and management of DSOs Objective system.

Defence Work Group Coordinators

- 40.0 Work Group Coordinators (WGC) are those Objective users who have volunteered to provide assistance to others in the use of Objective. They complete an advance level of training in the use of the system and have additional responsibilities in ensuring that information management within the system conforms to Defence and Commonwealth government policy and legislation.
- 41.0 Work Group Coordinators assist with the day-to-day management of files, documents and local system structures for their respective business areas. WGCs assist NWGCs carry out activities in maintaining ESD's Objective system. WGCs may also provide assistance to Contractor Objective Users if required.

Product & Service Managers (Defence Sponsors)

- 42.0 Defence Product and Service Managers (PSM) (refer Annex H) work closely with their respective Contractor representatives. Objective provides an important platform for the interchange of information between PSMs and Contractors which helps facilitate collaborative interactions.
- 43.0 PSMs, as the Defence Sponsor for Contractors, will help provide administrative oversight of Contractors' use of Objective. PSMs will help ensure that Objective is utilised appropriately by Contractor personnel with whom they deal and that the type and classification of documentation uploaded to the Objective system is appropriate.
- 44.0 Approval of document deliverables (in this case reports, plans, etc) by the PSM or the Contract Authority must continue as required under the contract; this includes the signing of the Deliverables Acceptance Certificate provided by the Contractor.

Contractor Work Group Coordinators

- 45.0 Contractors, in managing the information within Objective associated with their contract and in assisting their personnel who have access to Objective, require WGC trained personnel. Contractor WGCs (CWGC) will have the responsibility to add and delete Objective users, set access privileges, create and delete folders within their area of responsibility and troubleshoot basic Objective issues.
- 46.0 CWGCs will be required to liaise with Defence's NWGCs who may, from time-to-time, provide direction as to the appropriate management and maintenance of information within the system.

Table 2: Summary Contractor WGC Responsibilities

Objective/Folder Access	Contractor WGC Responsibility
Access to Objective	As a Contractor Sponsor - check and endorse Contractor Access Request Form – refer annex K. Stipulate access privileges for the User. If not a Contractor Sponsor, check and apply access privileges for Objective user.
Access to Estate Management Folders 1-7	Provide 'See and Open' access to respective Contractor users
Access to A Base Services Contractor - DEPOSIT BOX	Provide access and privileges to Contractor users for respective folders
Access to B Contract Administration Support – Change Contract Proposals	Request access via Contract Administration Support WGCs – Siwaporn Bundao or Jeff Schofield. Must have Defence sponsorship via PSM

Objective/Folder Access	Contractor WGC Responsibility
Access to C Defence Fuel Installation Documentation	DFI Documentation to be migrated into respective Property File in folders 03-07.
Access to D Estate and Facilities Services Project Documentation:	Request access via Janine Bent – National Workgroup Coordinator. Must have Defence sponsorship via PSM.

Contractor Sponsor

- 47.0 In conjunction with the procedure for accessing Objective, a representative for each Contractor is required to sponsor their employees' access to respective Objective folders and files. It is recommended that the Contractor Sponsor is also a CWGC.
- 48.0 The Contractor Sponsor is required to keep an up-to-date record of their employees who have access to Objective. The Contractor Sponsor is to ensure that users who no longer require access or have left their organisation are removed from the relevant systems. For Objective, this requires the Contractor Sponsor to notify a member of the NWGC group so that they may effect the removal of access and update Defence's access records. For removal of other system access, the Contractor Sponsor should follow the process for that system.

Contractor Objective User

- 49.0 Contractor Objective Users' (COU) within the Estate Management structure is determined at the individual level by the CWGC. The COU is expected to be responsible for the day-to-day management of documents into Objective in accordance with this instruction.
- 50.0 All Objective Users (Contractor or Defence) are responsible for notifying intended recipients within a timely manner of information uploaded to Objective for their use/reference. Whilst there is an 'alert' function within Objective, this is not to be relied upon for such notifications.

Getting access to the Defence Restricted Network and Objective

- 51.0 **Defence Restricted Network (DRN):** A user must have a Baseline or higher security clearance to gain access to the DRN. PSMs are to approve the request for contractor personnel to have access to the DRN account as the ('Defence Sponsor'). Details on how to go about doing this may be found through this link: [New DRN Accounts - electronic Network Access Request \(eNAR\)](#)
- 52.0 The eNAR process eliminates the need to complete paper-based forms. After the eNAR is submitted, it only takes approximately 30 minutes for a new DRN account to be available to the new user. At the end of the process, the new user will have the following:
- 52.1 A DRN account
 - 52.2 An E-mail account (including automatic inclusion on the relevant work site's email distribution list/s)
 - 52.3 Access to some software applications listed in the eNAR tool (if requested during the eNAR process)
 - 52.4 A personal storage area on their computer (H:\ drive)
- 53.0 **CAMPUS Online Training:** To obtain access to Objective the following courses must be completed through the DRN online training interface, CAMPUS. The full 'Objective User Training' takes approximately two hours to complete and consists of five modules.

- 54.0 **'Responsible Recordkeeping' - Course ID: 00002642 (Prerequisite)** - The aim of the Responsible Recordkeeping course is to deliver training in correct records management practice and to outline the records management policies and processes in place in the Australian Defence Organisation. The course is designed to enhance awareness of baseline recordkeeping responsibilities.
- 55.0 **'Objective User Training' - Course ID: 00004767 (refer annex I)** – The aim of Objective User Training is to provide trainees with basic knowledge and skill in the use of Defence's mandated record management system. This online course is supported by the Objective User Manual videos found on the Objective One-Stop-Shop intranet site.
- 56.0 Contractors have the ability to access CAMPUS Anywhere. CAMPUS Anywhere is an unclassified version of Campus that allows people from the Defence community to access corporate web-based training when not connected to the DRN (ie any internet-connected computer). DRN users are able to request a Campus Anywhere account by logging into Campus and selecting the Request Access link from the Campus Anywhere portal on the Homepage.
- 57.0 Not all Campus courses will be available on Campus Anywhere due to course content and links to DRN information. Unfortunately, at the time of producing this Instruction, Objective User training, Responsible Recordkeeping and Work Group Coordinator training is not available on CAMPUS Anywhere. An enquiry into this has recently been submitted. The current solution is to log on to a DRN terminal to undertake the CAMPUS training.
- 58.0 Upon completion of the 'Objective User Training' course, Users will be asked to complete an 'Objective User Account' activation web page (refer annex G). Within a few days of entering the details, the DRN Service Desk will create the new Objective account. In completing the activation web page, Contractors are asked to request that an abbreviation of their company name be included in their Objective identification – refer table 3. For example: Reynolds, David Mr 6 (DSRG – EMOS – TSA)

Table 3: List of Base Services Contractors and Objective Company ID

Contractor	Objective ID
Transfield Services (Australia) Pty Ltd	DSRG – EMOS – TSA
Spotless Facility Services Pty Ltd	DSRG – EMOS - SFS
Brookfield Global Integrated Solutions	DSRG – EMOS - BGIS
MSS Security	DSRG – MSP – MSS
Wilson Security	DSRG – MSP – WIL
Compass	DSRG – MSP - COM
Veolia	DSRG – MSP - VEO
DTZ (formerly United Group)	DSRG – MSP – DTZ
Augility	DSRG – MSP – AUG
Aurecon	DSRG – MSP - AUR

- 59.0 Once the Contractor has received confirmation of the activated Objective account via email, they will need to liaise with their Defence Sponsor (the PSM) to gain access to the relevant Estate Management Work Group folders in Objective.

- 60.0 The Contractor and Defence Sponsor will need to complete an **Objective Contractor Access Request form** (refer annex K) to request access to specific folders within the Estate Management folder area. Contractors will need approval from their Contractor Sponsor to access Objective. This form assists information managers in keeping track of Contractor users and security and access controls. Once the Objective Contractor Access Request form is completed, Contractors are to submit the form via email to ESD Data and Information Governance for action. The email address is DSRG-DSO.DDIG@defence.gov.au.
- 61.0 Defence Sponsors are to assist contractors requiring access to find a NWGC to implement the change on the system and sign-off on the access request. Defence NWGCs will be able to provide access and sign-off on Contractor access; however, it is expected that CWGCs will become proficient in the use of the system and manage their employees' access and privileges as necessary. This will provide Contractors with greater flexibility and management over their employees' access and activity within their folder areas. A list of Contractor WGC's who may approve Contractor employees' access will be provided once determined.
- 62.0 Once Objective user training has been completed, nominated Contractors may complete Objective Workgroup Coordinator training. This is a face-to-face course booked through Campus via the DRN intranet. This training provides users with greater detail about the functionality and use of Objective along with the Objective Work Group Coordinator Manual videos found on the Objective One-Stop-Shop site.

Section 3 – Digital Recordkeeping and Information & System Security

Digital Recordkeeping

- 63.0 Digital records are records created, communicated and/or maintained by means of computer technology. They may be ‘born digital’ (first created in electronic format) or they may have been converted into digital form from their original format (e.g. scans of hardcopy documents).
- 64.0 It is Australian Government policy to use digital recordkeeping to improve accessibility and reduce costs. Digital records must be stored in an approved recordkeeping system (i.e. Objective) and accessible for access requests under the *Archives Act 1983* and *Freedom of Information Act 1982*. Records must not be stored on uncontrolled or unapproved systems which include email, personal or network drives.
- 65.0 Defence and Contractors may not destroy original source records after copying, conversion or migration if:
- 65.1 the record is identified as Retain as National Archives (RNA) or Retain Permanently and is pre-1995 (these records must be transferred to National Archives of Australia (NAA) in original format);
 - 65.2 there is a legal requirement to retain the record in its original format or a specific format;
 - 65.3 there is a government policy, Executive Directive, NAA disposal freeze or Defence imposed embargo to not destroy the record;
 - 65.4 the record may be required as evidence in a current judicial proceeding or a future judicial proceeding that will be commenced, or will likely be commenced;
 - 65.5 the record is subject to a current application for access under the *Freedom of Information Act 1982*, *Archives Act 1983* or other legislation; and
 - 65.6 NAA has issued a notice that specifically requires retention of the record in its original format or a specific format.

Information and System Security Requirements

- 66.0 The security of information for both Contractors and Defence is an imperative part of daily business. The following information has been extracted from Defence policy as it relates to the use of information systems and information management. For up-to-date details on security within Defence please refer to Defence Security Manual as a starting point.
- 67.0 Defence personnel and external service providers are subject to the terms and conditions of their contract and are bound by security policy contained in the DSM and Information Security Manual (ISM). Failure to comply with the mandatory requirements of the DSM and ISM may result in action under the relevant contract provision or legislation.
- 68.0 Whilst there is much to keep abreast of in terms of Defence security, the following are some core policy rules specifically for DRN users. A DRN user must:
- 68.1 Not allow another person to use their log-on to access the DRN.
 - 68.2 Lock their screen when leaving their workstation whilst logged onto the DRN.

- 68.3 Not reveal their password (to any system or device) to another person.
- 68.4 Never record their Password anywhere.
- 68.5 Not store or transmit inappropriate material via the DRN.
- 69.0 When engaged in off-site work, including remote access, Defence personnel and external service providers must not allow people who are not appropriately cleared or do not have a need to know to view, overhear or otherwise access any official information which has not been authorised for public release.
- 70.0 A Data Spill is the introduction of information onto a network that is more highly classified than that for which the network is approved to store and process. Data Spills are classified as a major security incident due to the potential harm to national security that could result from unauthorised disclosure of classified information. All data spills are to be reported to a Security Officer in accordance with DSM Part 2:12 Security Incidents and Investigations.
- 71.0 Contractors accessing FOUO information will be required to have a Defence Industry Security Program (DISP) membership. For further information refer to DSM Part 2:42 Defence Industry Security Program.






User Groups (Workgroup Groups) and Work Group Coordinator Groups



- 72.0 User Groups are another way to help manage access and security within Objective. A Workgroup User Group is a collection of users assigned to a Work Group. WGCs are able to provide assistance in creating or modifying User Groups.
- 73.0 CWGC must not create or make requests for new Work Groups or Work Group Coordinator Groups in Objective via Objective Administrators unless first approved by the Director (or authorised representative) of DDIG.

Privileges

- 74.0 Privileges are the seven levels of permissions used to control access to objects in Objective – refer Table 4. Effectively applied privileges protect objects from unauthorised access. Privileges can be applied to objects (Work Groups, folders and files) to determine what tasks can be performed on those objects or on their contents. Privileges can be set at the user, Work Group, Folder, File or Object level.

Table 4: The Seven Levels of Permissions – Objective Icon and Privilege Descriptions

Action		Description
	See	The name of an object can be seen.
	Open	The selected object and its properties window can be opened.
	Create	Objects can be created within the structure, folder or file.
	Edit	A user can edit the attributes of an object and the content of electronic documents.
	Delete	An object can be deleted or moved.

	Security	A user with this privilege can assign others privileges to this object.
	Administrator	Objective Administrator. Assigned all privileges.

- 75.0 Objective's default access for folders and files is 'see and open'. In most cases, however, information which has a particular audience is 'locked down' to that audience so that other users are unable to see the information. Consistent with the 'need to know' principle within Defence, Objective users must not access files containing information which does not concern them or the work that they do. Audit trails within Objective identify all activity relevant to folders, files and documents.
- 76.0 Privileges to a hierarchy of workgroups and folders should be applied in a pyramid structure. The most limiting privileges are assigned to the highest workgroups and folders. The increased privileges are applied in order as the groups and users are allocated to specific folders and files within the Workgroup structure.

Section 4 – DEIS Business Rules

- 77.0 The following business rules define the data and document relationship within the DEIS. These rules specifically apply to information which is associated with IBIS (and later GEMS) and that which is stored in the Estate Management folders (1 – 7).
- 78.0 Each estate item must be classified against the Estate Register Information Model (ERIM) structure, and must be categorised as one of the following:
- 78.1 Region;
 - 78.2 Base Support Area;
 - 78.3 Property;
 - 78.4 Building;
 - 78.5 Building Level;
 - 78.6 Building Space;
 - 78.7 Infrastructure;
 - 78.8 Infrastructure System;
 - 78.9 Land Space;
 - 78.10 Equipment;
 - 78.11 Equipment System; or
 - 78.12 Hazard.
- 79.0 Each estate item must have a unique identifier (Estate ID) and each Estate ID must have one or more attributes that describes the estate item (refer to Estate Register Information Model Supplementary Information document). This is the Estate Master Data record.
- 80.0 Each Service Request (SR) registered in the EMOS, IBIS or GEMS systems must have a unique Service Request Number and each SR can have a minimum of one or more Work Orders (WO). Each WO must be uniquely identified and be associated with an Estate Item at the lowest possible level in the ERIM hierarchy. For example, if a service request is logged for an air conditioning problem it should be associated with the equipment item not the building. Noting the initial request may have the SR associated to a higher level estate item until the actual item is identified by the Contractor.
- 81.0 Each document registered in Objective must have a unique document ID (Objective ID) and it must include in the document name the Estate ID if it relates to or is associated with an estate item.
- 82.0 Where an Objective ID is related to an estate record they must be “linked” and the Objective ID entered in against the estate record held in the Contractor’s system, IBIS and GEMS.
- 83.0 Where the Objective ID is a result of a SR or a WO, the Objective ID must reference the unique SR or WO ID. All documents registered in Objective must conform to the correct naming standard allocated to the document class (type), per the current document.
- 84.0 If documents need to be visible within a 12 hour timeframe, they are to be uploaded and registered via the Deakin Objective Server (dknrdm02). Document recipients must log into this server to view the uploads.

85.0 For Base Services Contractor documentation, the details of each document registered in Objective must be captured through the submission of an IDS record in accordance with IDS DS.ALL.80.01 - Documentation Update.

Acceptable File Types

Business Rules

86.0 Passwords must not be applied to documentation for any reason unless expressly agreed to in writing by DDIG.

87.0 The following file types are acceptable:

File Type	Comments
Word Version 2003 or higher	
Excel Version 2003 or higher	
MS Project 2003 or higher	
MS Outlook 2003 or higher.	Email records when stored in Objective must include both the email body and any attachments. Where an email 'trail' is captured retrospectively, only the last email in the trail (containing all the previous emails in the conversation) should be captured. If another email thread is started containing only some of the initial email threads then the subsequent threads should also be captured even if there is some duplication of content.
MS Visio 2003 or higher	
Adobe Portable Document Format (PDF)	For all PDF documents, all text should have Optical Character Recognition (OCR) applied. When providing PDF reports over 20 pages in length, apply Bookmarks to assist with navigation through the document. Files should be optimised where the reduction in file size does not affect the print quality or the ability to interrogate the content. Where feasible, native files should be provided along with PDF drawings, maps and plans.
Plans, maps and other spatial information.	Must be provided in accordance with the Spatial Data Management Plan (SDMP).

File Type	Comments
ZIP Files	<p>Acceptable method for reducing file size for transmission and can be opened on the DRN.</p> <p>Documents within Zip files must be extracted and placed in Objective individually.</p>

Document Scanning

- 88.0 Refer to Defence policy regarding minimum document scanning specifications required for all post-1995 records and pre-1995 temporary records. Destruction of physical records that have been digitised may only be performed in accordance with General Records Authority 31 (GRA 31).
- 89.0 Optical character recognition (OCR) is best practice and should be used for all documents containing text unless there is a specific business case against it. The OCR rendition of a record should be captured and managed in addition to, but not instead of the scanned images.
- 90.0 Defence has scanning metadata capture specifications which meets metadata requirements regarding process and methodology for records used in evidence. If scanning directly into Objective the metadata will be automatically captured, and tested using the Objective Desktop Scanning Tool. Chief Information Officer Group is responsible for managing the additional metadata script required for all digitisation projects on the Defence Restricted Network and Defence Secret Network.

Imagery

- 91.0 To ensure that all Defence imagery maintains the highest possible value it must be controlled by standardised handling procedures and tagged with appropriate metadata.
- 92.0 DEF(AUST) GEO 7100 PART A defines the metadata standard for Hand Held Imagery (HHI). This metadata provides information relating to specific attributes of the image. The creator or originator of the image is responsible for capturing the specific metadata attributes.
- 93.0 Where there is no capability to have a recordkeeping metadata schema that allows for sentencing under the *Archives Act 1983* or the ability to integrate with one, the database must be catalogued in an approved recordkeeping system. In addition to standard recordkeeping data, the catalogue entry for the HHI file must contain, as a minimum, metadata regarding the location, custodianship and accessibility of the HHI and a synopsis of the types of HHI the file contains.
- 94.0 Motion Imagery (MI) is imagery utilising sequential or continuous streams of images that enable observation of the dynamic behaviour of objects within the scene. Guidance for the management of Defence MI, including legacy MI, is found in DEF(AUST) GEO 7101. It comprises two parts: PART A describes the handling procedures for MI and PART B defines the metadata standards for MI.

Uploading Documents to Objective and Digital Storage Devices

Filing Documents in Objective

- 95.0 Annex M provides a list of document descriptors (for use in file naming convention – refer items 107 and 108) and guidance on where such types of documents will be placed and which stakeholder groups are likely to need visibility.

General Uploads to Objective

- 96.0 Defence's DRN terminals do not allow drives, optical or magnetic media and other peripheral computing hardware devices unless they are Defence approved. This type of equipment must be appropriately managed and maintained and the facilities storing the equipment must protect the records and make them accessible.
- 97.0 Contractors may use CD or DVD discs to 'burn' documents to and from Objective and some terminals have scanners directly linked and available for use.
- 98.0 Digital storage devices deteriorate with time and use and are susceptible to dust and fluctuations in humidity, temperature and radiation. It is therefore important to ensure that stable environmental conditions are maintained. Software changes may also require format conversion to ensure that information remains accessible.

Defence Email

- 99.0 Files received by DRN email are limited to a file size of 5MB and each Mailbox is limited to a maximum capacity of 900MB, after which point the Mailbox will not receive or transmit email messages.

External File Servers Downloads

- 100.0 Information downloaded from an external file or web server for example, Dropbox or Send-It, is held to the same provisions as external email; it is limited to information that is UNCLASSIFIED. An appropriate business case may be required to access some file servers beyond the Defence firewall.

CD and DVDs

- 101.0 Defence DRN terminals are able to read both CDs and DVDs and copy files from the disks to the Desktop or DRN. Most terminal disk drives are able to write to CDs however not all have DVD write permissions.
- 102.0 If not enabled to burn files from the DRN, DVD/CD burning for file backup may be requested by using the Service Request Catalogue.

Portable Electronic Devices – USB read-only multi-card reader

- 103.0 **Portable Electronic Devices (PEDs)** are devices that can process, store or communicate information electronically. Most PEDs also contain media, which may be removable or fixed within the device. Examples of PEDs that may be found within Defence include but are not limited to:
 - 103.1 laptops, tablets, eReaders, phones, cameras, audio players/recorders;
 - 103.2 data transfer and format converters, that transfer information between peripherals without the use of an intervening computer, such as portable Wi-Fi hotspots, one touch backup drives, Serial Advanced Technology Attachment (SATA) hard disk to Universal Serial Bus (USB) converters and USB host transfer devices; and
 - 103.3 cordless telephones such as Digital Electronic Cordless Telecommunications (DECT) phones and other wireless protocols including WiFi.
- 104.0 PEDs and media are to be afforded a level of protection commensurate with the classification of information they process or store and will be used in a way that will not compromise the official information or the security of ICT systems.
- 105.0 Policy for using PEDs outside of the office, conducting remote access to Defence systems from both privately owned and Defence controlled devices may be found in DSM Part 2:21 Off-Site Work.

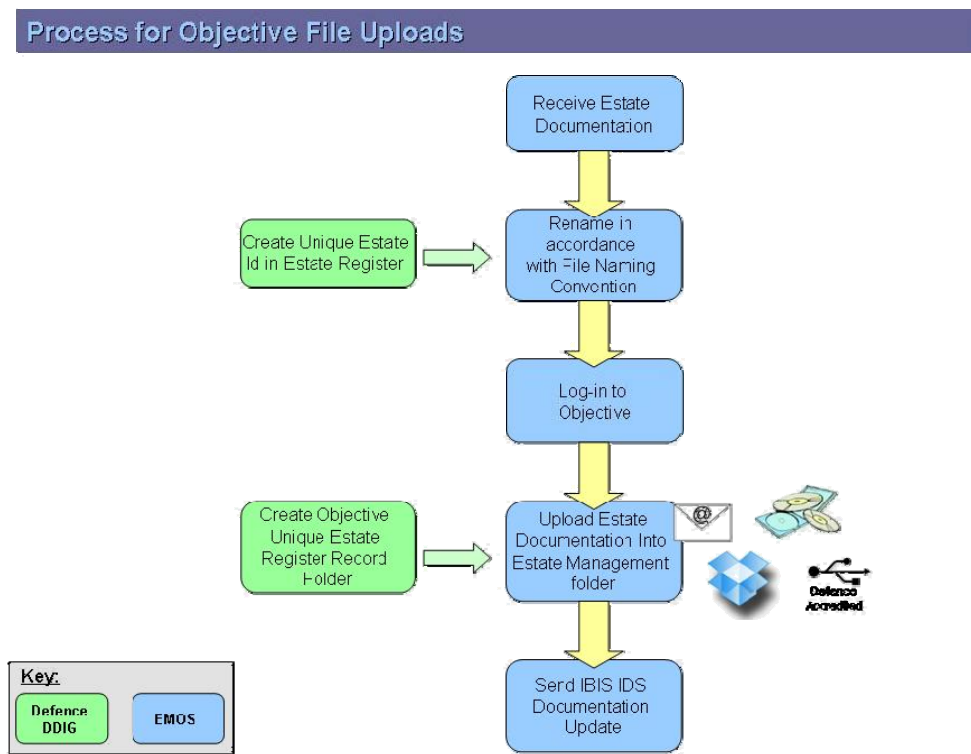
- 106.0 A USB Read-only Multicard Reader facilitates the upload only of information from portable devices to the DRN. Users can upload appropriate data from personal devices (eg Digital Camera's, Digital Voice recorders) that store data on removable flash memory cards such as SD, MicroSD and compact flash to the DRN. More information may be found on the Defence ICT intranet.

USB Sticks and Portable Hard Drives

- 107.0 A USB thumb drive is a small device used to transfer files between electronic equipment/media devices or networks. A thumb drive may also be called Flash Drive, Pen Drive, Thumbnail Drive, USB Thumb Drive, Memory Stick, Micro Drive, Micro USB, and Zip Drive.
- 108.0 Only Defence accredited Portable Storage Devices may be used on DRN Terminals. The Defence Kanguru Defender 2000 (4GB) USB Thumbdrives are approved on Defence networks that are PROTECTED or below including the DRN.
- 109.0 The Defender 2000 should work on all workstations without further configuration. These drives can be purchased via Staples, Product Code: 18965646. User Registration forms are not to be completed or returned to Kanguru.
- 110.0 USB users must obtain, manage and use Defence supplied Kanguru Defender 2000 USB drive in accordance with applicable Defence IT policies.
- 111.0 To acquire an approved USB thumb drive for the purposes of this Operating Instruction, send an email requesting a USB thumb drive and including the name, phone number and email address of the responsible person(s) to your Contract Authority mailbox, CC'ing DSRG-DSO.DDIG@defence.gov.au. The Contract Authority will purchase a Defence approved USB drive from Staples. The Contract Authority will provide a letter to the contractor requiring signing for the USB drive and agreeing terms of use as per policy and CIOG site. The USB drive must be returned to the Contract Authority when use has finished.

Objective to IBIS

112.0 The following flow diagram provides an overview of the process for uploading Estate Management documentation (folders 1 – 7) to IBIS via Objective.



Documents / Records Generated Under Base Services Contracts

113.0 The EMOS Contract Authority has developed a Reports and Plans Deliverables (RPD) Register for PSMs, Contractors and CAs showing the list of documents required under the Contract, when they are due and who the key recipient is for that document. A column has been included in this register to indicate where the RPD should be placed in Objective when submitting, reviewing and/or transferring the document(s). This is currently being populated.

File Naming Convention

114.0 In general, Objective's file naming convention provides that:

- 114.1 all object titles in Objective are written in title case, for example: Remembrance Day Ceremonial Parade
- 114.2 commas, colons and semi colons must not be used in a title;
- 114.3 hyphens can be used in titles;
- 114.4 abbreviations and acronyms should be written in full;
- 114.5 classification caveats must not be used in a title;
- 114.6 file names must be logical and detailed;
- 114.7 file titles must not contain sensitive information (such as personal details);

- 114.8 all file names must be unclassified;
- 115.0 For Estate related documentation which is placed in the Estate Management, folders 1 – 7, the following naming convention will apply:
- [Unique Property ID]<>[Document Type]<>[Document Date]-<>[BSC Unique Identifier] Eg: 1012/A011 Fire Safety Survey 20150219-S0385**
- 116.0 **Unique Property ID** – this ID can be found in the IBIS Estate Register via the DRN Online Portal or in the Estate Register extract provided to Base Services Contractors under the Attribute 1035.
- 117.0 **Document Type** – document descriptions are taken from the IBIS Allowed Values List “ALL.AVL.41 Document Type”. Acronyms for each are found at Annex M. Where the acronym is generic, additional descriptive words may be included, for example, Business Case is one descriptor, BC is its acronym; however, for the file name to become more meaningful it could be adapted to ‘BC - New Generators’. Folders for each unique Estate Register Item will be created upon request by Defence.
- 118.0 **BSC Unique Identifier** – at the request of BS Contractors, this provides for an identifier for tracking of documents in BS Contractor systems. It does not need to be populated and is not parsed by Defence. Defence do not need to use this when placing documents in the EM folder.
- 119.0 **Document date** – is the date which the document has been provided to Defence.
- 120.0 Objective allows duplicate files names because each object has a unique identifier. All documents in the EM area – folders 1 – 7 which link with IBIS will be required to have the same naming convention as identified above.

Metadata requirements for records in Objective

- 121.0 All digital Defence records must comply with the metadata standards described in the Australian Government Recordkeeping Metadata Standard 2.0 (AGRkMS).
- 122.0 For Estate related documentation which links with IBIS, custom metadata catalogues for Objective files are currently being investigated. It is envisaged that once criteria has been determined, creation of the catalogues will take approximately six months.
- 123.0 See Annex N for metadata requirements based on existing Objective metadata fields.

Section 5 - System Support – Useful Links

- 124.0 Objective Online Support – log a request via the Service Request Catalogue
- 125.0 Objective User Account Request
- 126.0 Objective One-Stop-Shop
- 127.0 Objective User and WGC Manuals: Refer to the One-Stop-Shop "Resources" tab
- 128.0 Objective Training Enquiries / Nominations Refer to the One-Stop-Shop "Training"
- 129.0 Objective Help-desk – in addition to being able to log a request/service job via the ICT online portal, telephone enquiries may be made by calling 133 272
- 130.0 Records Management Policy Intranet Site
- 131.0 Defence Public-Key Infrastructure (PKI) - Defence Internet
- 132.0 Defence Public Key Infrastructure - Defence Intranet - CIOG
- 133.0 Digital Signatures - Benefits
- 134.0 Contractor access and process queries for the Estate Management folder area, please contact one of the National WGC identified in Annex A.

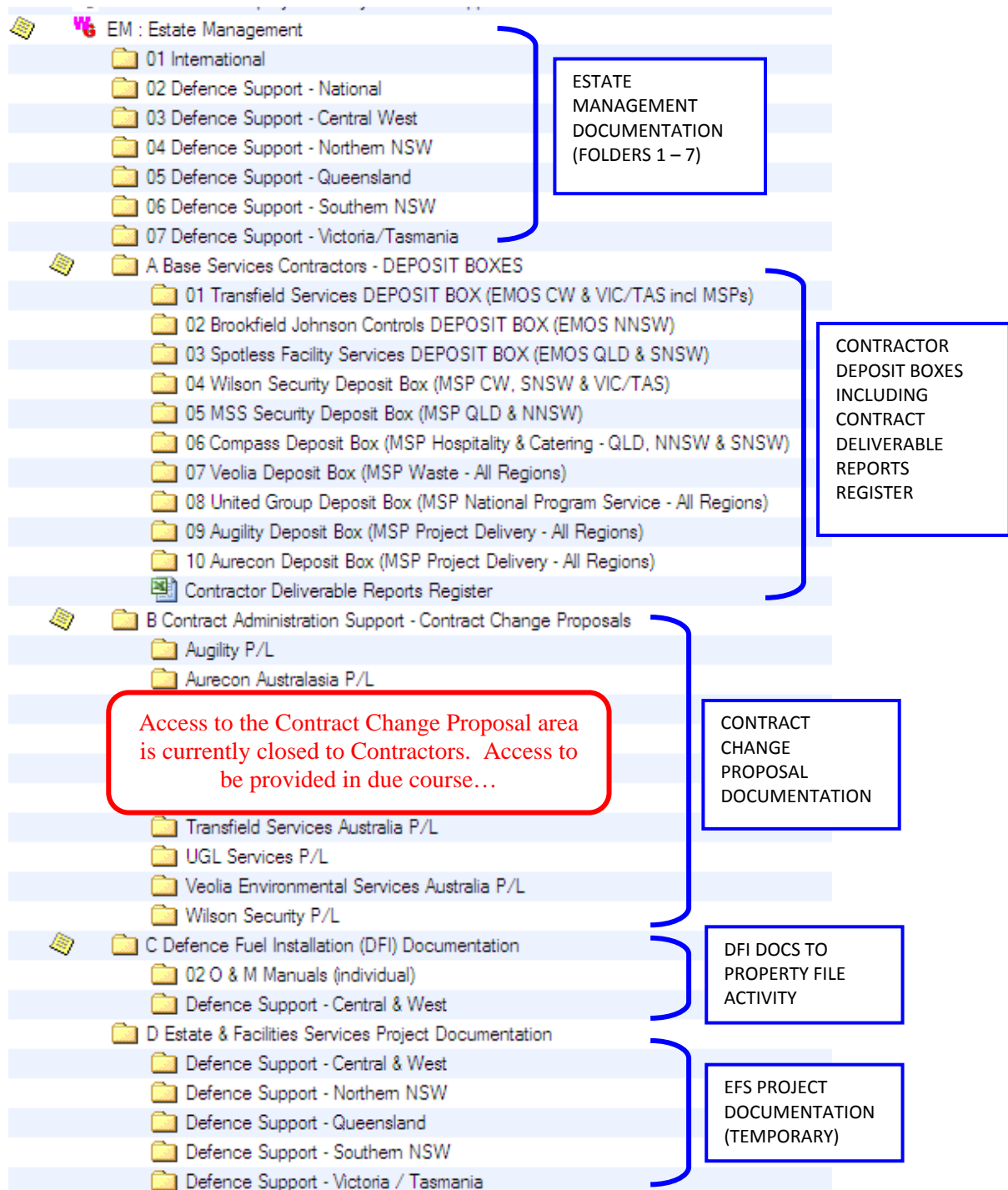
Annex A - Estate Management Folders, Intended Use, Ownership and Key Stakeholders

	Typical Use of Folders	Key Stakeholders	Default Access	Folder Ownership	Defence WGC
Estate Management Documentation (Folders 1 – 7)	Storage of Estate Related documentation connecting with IBIS / GEMS systems	All BSR Contractors , Infrastructure Division, Estate Works Program Office, DSRG Personnel	Open access to all Contractors and Defence Personnel	Directorate of Data and Information Governance	Mr Jeff Schofield/ Mr Michael Kovacs
Contractor Deposit Boxes	Transfer of Contract related / associated information Includes area for ECART Monthly Reporting and Contract Deliverables Reports and Plans	Contractors, PSMs, CAs	Restricted to individual Contractors, PSMs, CAs and other Defence stakeholders as necessary	EMOS Contract Authority	Ms Jennifer Commegno / Mr David Stint/Mr Jeff Schofield
Contract Change Proposals	Facilitate Contract Change Proposal process	Contractors, CAS, PSMs, CAs	Restricted to individual Contractors, PSMs, CAs and other Defence stakeholders as necessary	Contract Administration Support (Directorate of Contract Governance)	Ms Siwaporn Bundao / Mr Jeff Schofield
Defence Fuel Installation	Document migration activity to relevant Property File underway.	N/A	N/A	N/A	Jeff Schofield
Estate and Facilities Services – Project Documentation (interim folder)	Temporary storage location for project documentation historically maintained by EFS – may need transferring to the Estate Management Documentation (Folders 1 – 7)	Regional EFS, NPS/PDS, Estate Upkeep, Estate Works Program Office Contractors, Infrastructure Division	Open access to all Contractors and Defence Personnel	Regional Estate and Facility Services	Ms Janine Bent/Mr Jeff Schofield

Annex B – Defence National Work Group Coordinators

First Name	Last Name	Objective Id	Region	Position	Directorate	Email	Telephone
Jennifer	Commegno	uD3271	Central & West	Contract Manager - EMOS Contract Authority	Directorate Base Services Management Integration & Coordination	jennifer.commegno@defence.gov.au	08 7383 0419
Andrew	Clough	uA15841	Central & West	RIM - Estate & Facility Services Central & West	Estate & Facility Services Central & West	andrew.clough@defence.gov.au	08 7383 0374
Fred	Grocke	uD1429	Central & West	Customer Services Manager - SA	Defence Support - SA	fred.grocke@defence.gov.au	08 7383 3008
Brian	Holland	uA16566	Central & West	Defence Records Management - SA	Defence Support - SA	brian.holland@defence.gov.au	08 7389 6493
Jeff	Schofield	uG2812	Northern NSW	Information Manager - DS-NNSW	Defence Support - NNSW	jeff.schofield@defence.gov.au	02 4034 7666
Janine	Bent	uL155	Southern NSW	Regional Corporate Information Manager - RMV	Defence Support - RMV	janine.bent@defence.gov.au	02 6055 2161
Michael	Kovacs	uX28792	Northern NSW	Data Compliance Officer - DS-NNSW	Directorate Data & Information Governance	michael.kovacs@defence.gov.au	02 9393 2426
Sandra	Sumpton	uA28765	Queensland	Customer Service Officer	Defence Support - QLD	sandra.sumpton1@defence.gov.au	07 3332 6400
Siwaporn	Bundao	uK358	Northern NSW	Contract Administrator	Directorate Contract Governance - Contract Administration Support	siwaporn.bundao@defence.gov.au	02 9393 2043
Katherine	Butler	uR2489	Branch	EA to HDSO	Head Estate Services Division	katherine.butler@defence.gov.au	02 6265 6138
Ruihana	Hepi	uR1932	Branch	Executive Officer - Estate Support	Estate Support	ruihana.hepi@defence.gov.au	02 6266 2891
Janelle	Gilbert	uQ418	Branch	Executive Assistant to DGBPESP	Directorate Base Planning, Engagement and Service Performance	janelle.gilbert1@defence.gov.au	02 6266 4942
Christine	Amos	uA25100	Northern NSW	Information Coordinator	Defence Support - Northern NSW	christine.amos2@defence.gov.au	02 4034 8338
John	Vanderdonk	uC1640	Central & West	Contract Officer	Directorate Base Services Management Integration & Coordination	john.vanderdonk1@defence.gov.au	08 9311 2235
Mira	Kovac	uR3675	Vic / Tas	Regional Integration & Coordination Officer	Regional Integration & Coordination - Vic/Tas	mira.kovac@defence.gov.au	03 9282 3609
David	Stint	uD6016	Central & West	Contract Administration Officer	Directorate Base Services Management Integration & Coordination	david.stint1@defence.gov.au	08 7383 0160








Annex C - Estate Management Folder Structure



Example Only - Zoom In to see detail

Level 3 Navigational	Level 4 Navigational	Level 5 Navigational	Level 6 Functional	Level 7 Functional	Level 8 Operational	Container Type	Defence Work Group Coordinator Folder Ownership	Contractor Information Manager / POC	User Groups	Access / Privilege Level	
W6 Estate Management Workgroup						Work Group					
	01	International	IBIS Estate Management Document Folders 1 - 7			Folder	Directorate Data & Information	All DSO (Incl BS Contractors)		✓✓✓✓✓	
	02	National					Folder	Directorate Data & Information	All DSO (Incl BS Contractors)		✓✓✓✓✓
	03	Northern NSW					Folder	Directorate Data & Information	All DSO (Incl BS Contractors)		✓✓✓✓✓
	04	Queensland					Folder	Directorate Data & Information	All DSO (Incl BS Contractors)		✓✓✓✓✓
	05	Southern NSW					Folder	Directorate Data & Information	All DSO (Incl BS Contractors)		✓✓✓✓✓
	06	Victoria & Tasmania					Folder	Directorate Data & Information	All DSO (Incl BS Contractors)		✓✓✓✓✓
	07	Central & West					Folder	Directorate Data & Information	All DSO (Incl BS Contractors)		✓✓✓✓✓
	A	Base Services Contractors - Deposit Boxes				Folder	Jen Commegno / David Stint	Contractors, Relative PSMs and CA		✓✓✓✓✓	
	1.0	Transfield Services Deposit Box				Folder	Jen Commegno / David Stint	Transfield Only, Relative PSMs and CA		✓✓✓✓✓	
	1.1	MIC				Folder	TBC - PSM (Interim J Commegno)	Transfield Only, Relative PSMs and CA		✓✓✓✓✓	
	1.2	BSSC				Folder	TBC - PSM (Interim J Commegno)	Transfield Only, Relative PSMs and CA		✓✓✓✓✓	
	1.3	Commercial Ops				Folder	TBC - PSM (Interim J Commegno)	Transfield Only, Relative PSMs and CA		✓✓✓✓✓	
	1.4	Special Forces Training				Folder	TBC - PSM (Interim J Commegno)	Transfield Only, Relative PSMs and CA		✓✓✓✓✓	
	1.5	Training Areas and Range Management				Folder	TBC - PSM (Interim J Commegno)	Transfield Only, Relative PSMs and CA		✓✓✓✓✓	
	1.6	Transport				Folder	TBC - PSM (Interim J Commegno)	Transfield Only, Relative PSMs and CA		✓✓✓✓✓	
	1.7	Airfield Ops				Folder	TBC - PSM (Interim J Commegno)	Transfield Only, Relative PSMs and CA		✓✓✓✓✓	
	1.8	Estate Upkeep				Folder	TBC - PSM (Interim J Commegno)	Transfield Only, Relative PSMs and CA		✓✓✓✓✓	
	1.9	Laundry & Drycleaning				Folder	TBC - PSM (Interim J Commegno)	Transfield Only, Relative PSMs and CA		✓✓✓✓✓	
	1.10	Land Management				Folder	TBC - PSM (Interim J Commegno)	Transfield Only, Relative PSMs and CA		✓✓✓✓✓	
	1.11	Pest & Vermin				Folder	TBC - PSM (Interim J Commegno)	Transfield Only, Relative PSMs and CA		✓✓✓✓✓	
	1.12	Cleaning				Folder	TBC - PSM (Interim J Commegno)	Transfield Only, Relative PSMs and CA		✓✓✓✓✓	
	1.13	Housekeeping				Folder	TBC - PSM (Interim J Commegno)	Transfield Only, Relative PSMs and CA		✓✓✓✓✓	
	1.14	Base Reprographics				Folder	TBC - PSM (Interim J Commegno)	Transfield Only, Relative PSMs and CA		✓✓✓✓✓	
	1.15	Sport & Recreation				Folder	TBC - PSM (Interim J Commegno)	Transfield Only, Relative PSMs and CA		✓✓✓✓✓	
	1.16	H & C				Folder	TBC - PSM (Interim J Commegno)	Transfield Only, Relative PSMs and CA		✓✓✓✓✓	
	1.17	Rescue & Fire Fighting				Folder	TBC - PSM (Interim J Commegno)	Transfield Only, Relative PSMs and CA		✓✓✓✓✓	
	1.18	Aircraft Refuelling				Folder	TBC - PSM (Interim J Commegno)	Transfield Only, Relative PSMs and CA		✓✓✓✓✓	
	1.19	POL				Folder	TBC - PSM (Interim J Commegno)	Transfield Only, Relative PSMs and CA		✓✓✓✓✓	
	1.20	Retail Stores				Folder	TBC - PSM (Interim J Commegno)	Transfield Only, Relative PSMs and CA		✓✓✓✓✓	
	1.21	ECART - EMOS Contract Authority Reporting Tool				Folder	TBC - PSM (Interim J Commegno)	Transfield Only, Relative PSMs and CA	✓✓	✓✓✓✓✓	
	2.0	Spotless Facility Services Deposit Box				Folder	Jen Commegno / David Stint	Spotless Only, Relative PSMs and CA		✓✓✓✓✓	
	3.0	Brookfield Johnson Control Deposit Box				Folder	Jen Commegno / David Stint	BJC Only, Relative PSMs and CA		✓✓✓✓✓	
	4.0	Compass Deposit Box				Folder	TBC (Interim J Commegno)	Compass Only, Relative PSMs and CA		✓✓✓✓✓	
	5.0	Wilson Security Deposit Box				Folder	TBC (Interim J Commegno)	Wilson Only, Relative PSMs and CA		✓✓✓✓✓	
	6.0	MSS Security Deposit Box				Folder	TBC (Interim J Commegno)	MSS Only, Relative PSMs and CA		✓✓✓✓✓	
	7.0	Veolia Deposit Box				Folder	TBC (Interim J Commegno)	Veolia Only, Relative PSMs and CA		✓✓✓✓✓	
	8.0	United Group Deposit Box				Folder	TBC (Interim J Commegno)	United Group Only, Relative PSMs and CA		✓✓✓✓✓	
	9.0	Augility Deposit Box				Folder	TBC (Interim J Commegno)	Augility Only, Relative PSMs and CA		✓✓✓✓✓	
	10.0	Aurecon Deposit Box				Folder	TBC (Interim J Commegno)	Aurecon Only, Relative PSMs and CA		✓✓✓✓✓	
	B	Contract Administration Support - Contract Change Proposals				Folder	Swaporn Bundao / Jeff Schofield	Contractors, CAS, DPCB, Relative PSMs and CA		✓✓✓✓✓	
		Transfield Services Deposit Box				Folder	Swaporn Bundao / Jeff Schofield	Transfield Only, CAS, Relative PSMs and CA		✓✓✓✓✓	
		Spotless Facility Services Deposit Box				Folder	Swaporn Bundao / Jeff Schofield	Spotless Only, Relative PSMs and CA		✓✓✓✓✓	
		Brookfield Johnson Control Deposit Box						BJC Only, Relative PSMs and CA		✓✓✓✓✓	
		Compass Deposit Box						Compass Only, Relative PSMs and CA		✓✓✓✓✓	
		Wilson Security Deposit Box						Wilson Only, Relative PSMs and CA		✓✓✓✓✓	
		MSS Security Deposit Box						MSS Only, Relative PSMs and CA		✓✓✓✓✓	
		Veolia Deposit Box						Veolia Only, Relative PSMs and CA		✓✓✓✓✓	
		United Group Deposit Box				Folder	Swaporn Bundao / Jeff Schofield	United Group Only, Relative PSMs and CA		✓✓✓✓✓	
		Augility Deposit Box				Folder	Swaporn Bundao / Jeff Schofield	Augility Only, Relative PSMs and CA		✓✓✓✓✓	
		Aurecon Deposit Box				Folder	Swaporn Bundao / Jeff Schofield	Aurecon Only, Relative PSMs and CA		✓✓✓✓✓	
	C	Defence Fuel Installation (DFI) Documentation				Folder	John Vander Donk / Jen Commegno	All DSO (Incl BS Contractors)	✓✓✓✓✓	✓✓✓✓✓	

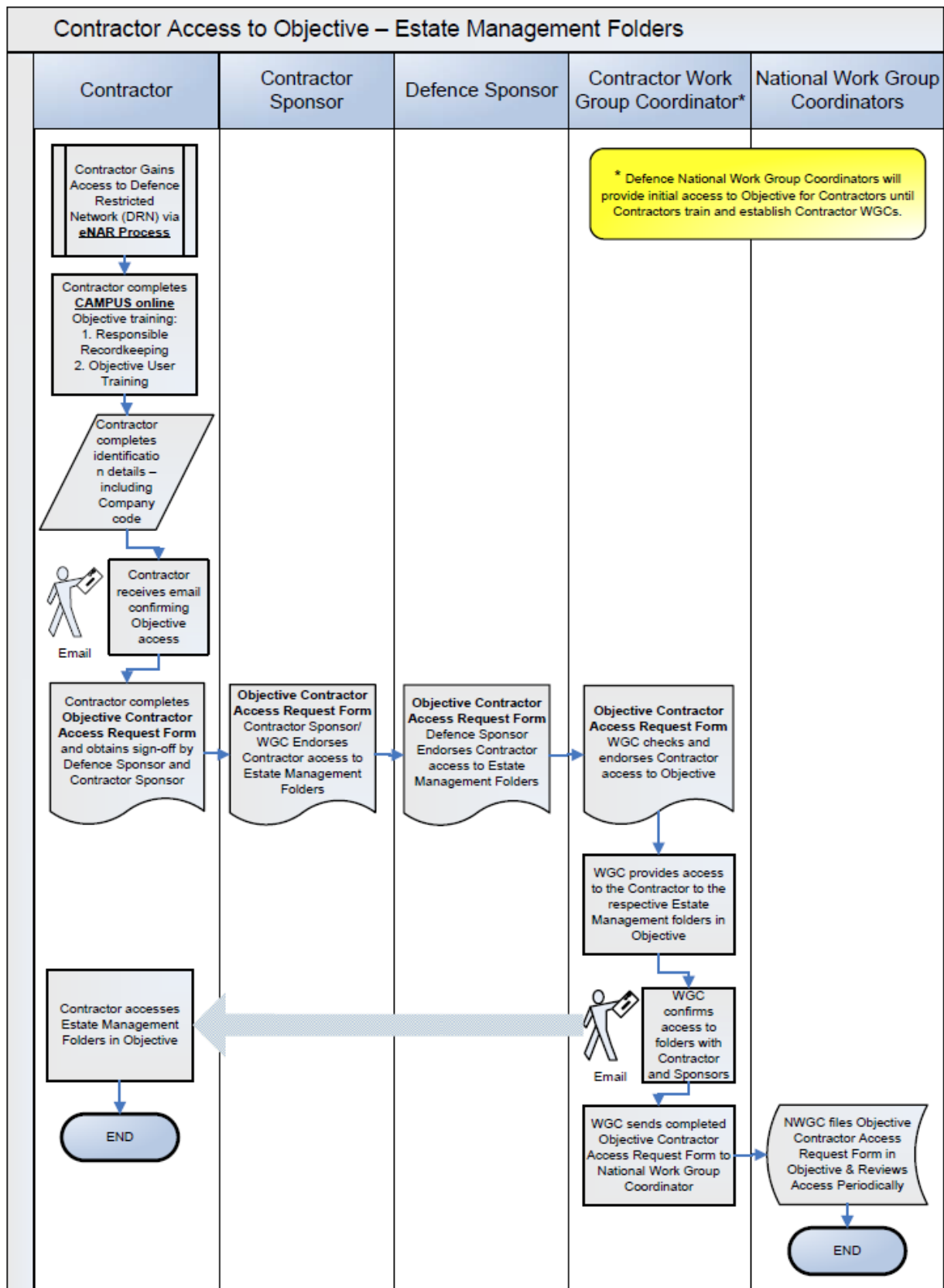
Annex E – Estate Management Folders, Folder Owners and Purpose of Folder Area

Level 3	Level 4	Level 5	Level 6	Level 7	Level 8	Container Type	Work Group Coordinator	Folder Ownership	Comments
Navigational	Navigational	Navigational	Functional	Functional	Operational			     	
 Estate Management Workgroup						Work Group	Defence: Jen Commegno / Andrew Clough		This Work Group folder and sub-folders '01 to '07 have been set up for the storage of Estate documentation requiring linkage to IBIS. Default Access to these folders '01 to '07 should be set at 'See Open' for all Objective Users. DDIG is the owner of these folders and are responsible for creating, modifying and deleting information in this area of the Estate Management folder. Contractor WGCs will not have privileges to make these changes.
	01	International				Folder		DDIG	
	02	National				Folder		DDIG	
	03	Northern NSW				Folder		DDIG	
	04	Queensland				Folder		DDIG	
	05	Southern NSW				Folder		DDIG	
	06	Victoria & Tasmania				Folder		DDIG	
	07	Central & West				Folder		DDIG	
	A	Base Services Contractors - Deposit Boxes				Folder	Defence: Jen Commegno / Dave Stint		These folder areas are set up for each Base Services Contractor to transfer information between Contractors and Defence which do not need to be placed in the other areas of the Estate Management folder structure. Contractor WGCs are responsible for managing the information, structures and access within their organisation's Work Group. Defence National Workgroup Coordinators also have access to make changes within these folders, however, this will be done in consultation with the respective Contractor WGC. Overall, DDIG is the owner of these folders and reserves the right to make whatever changes, restrictions, etc deemed necessary in meeting Defence information management needs.
		01	Transfield Services Deposit Box			Folder	Contractor TBA (Defence: Jen Commegno / Dave Stint)		
		02	Spotless Facility Services Deposit Box			Folder	Contractor TBA (Defence: Jen Commegno / Dave Stint)		
		03	Brookfield Johnson Control Deposit Box			Folder	Contractor TBA (Defence: Jen Commegno / Dave Stint)		
		04	Compass Deposit Box			Folder	Contractor TBA (Defence: Jen Commegno / Dave Stint)		
		05	Wilson Security Deposit Box			Folder	Contractor TBA (Defence: Jen Commegno / Dave Stint)		
		06	MSS Security Deposit Box			Folder	Contractor TBA (Defence: Jen Commegno / Dave Stint)		
		07	Veolia Deposit Box			Folder	Contractor TBA (Defence: Jen Commegno / Dave Stint)		
		08	United Group Deposit Box			Folder	Contractor TBA (Defence: Jen Commegno / Dave Stint)		
		09	Augility Deposit Box			Folder	Contractor TBA (Defence: Jen Commegno / Dave Stint)		
		10	Aurecon Deposit Box			Folder	Contractor TBA (Defence: Jen Commegno / Dave Stint)		
	B	Contract Administration Support - Contract Change Proposals				Folder	Siwaporn Bundao/Jeff Schofield		Contract Administration Support currently provide this folder area for PSMs and CAs. Once Contractor access is determined, they too may have access to their specific CCPs.
	C	Defence Fuel Installations				Folder	John Vanderdonk / Jen Commegno		DFI documentation being migrated into relevant Property File. DFI Folder structure to be removed once completed.
	D	Estate and Facility Services Project Documentation				Folder	Janine Bent		This is an interim folder for EFS Project Documentation - predominantly for Defence use until a permanent location is identified for this information. Contractors may have access to this information upon request via Janine Bent (WGC)

Annex F – Estate Management Folders (1 – 7) – Folder Hierarchy

▼	EM : Estate Management
▶	01 International
▶	02 Defence Support - National
▼	03 Defence Support - Central West
▶	BSA-Berimah
▶	BSA-Darwin
▼	BSA-Edinburgh Defence Precinct
▶	0307-Edinburgh Parks
▶	0660-Uro Bluff PAWP telemetry site
▶	0661-Penfield (Transferred to 0939)
▶	0939-RAAF Base Edinburgh
▶	0940-Mt Lofty Transmitting Station (Leased)
▶	1073-DSTO - Edinburgh
▶	1077-Vacant land - Heaslip Rd Penfield adj RAAF Base Edinburgh
▼	1098-Defence Establishment Woomera
▶	Building
▼	Equipment
▶	1098-EZ003-Freshwater Reticulation
▶	1098-T0078-20 ton Weighbridge (509965)
▶	SA-E23177-Crane - Tadano Crane (Vehicle)
▶	SA-E7461-Street & Walkway Lighting x 456
▶	Equipment System
▶	Infrastructure
▶	Infrastructure System
▶	Land Space
▶	1110-St Kilda Transmitting Station
▶	1118-Jindalee Receiver Site - MT Everard
▶	1119-Jindalee Transmitting Site - Harts Range
▶	3060-Thistle Island (Leased)
▶	3120-Cheetham Salt Works (Leased land)
▶	3149-Instrument Landing System (ILS) Middle Marker (Leased)
▶	3150-Instrument Landing System (ILS) Outer Marker (Leased)
▶	3246-O-Outer Harbour (Berth # 8)
▶	3314-DSI-TA
▶	3393-TX Australia Pty Ltd Telecommunications tower
▶	BSA-FBW
▶	BSA-Larrakeyah
▶	BSA-MARS
▶	BSA-MPRS
▶	BSA-NT-K Property Officer
▶	BSA-Pearce
▶	BSA-Robertson
▶	BSA-Tindal
▶	04 Defence Support - Northern NSW
▶	05 Defence Support - Queensland
▶	06 Defence Support - Southern NSW
▶	07 Defence Support - Victoria/Tasmania
▼	A Base Services Contractors - DEPOSIT BOXES
▼	01 Transfield Services DEPOSIT BOX (EMOS CW & VIC/TAS incl MSPs)

Annex G – Flowchart: Contractor Access to Objective– Estate Management Folders



Annex H – Product and Service Line Matrix – Contract Authorities, Contractors and PSMs


Service Lines	Central & West	DS QLD	DS NNSW	DS SNSW	VIC / TAS	CA Region	CA	PSM Region	PSM
MIC (incl Estate Appraisal)	Transfield	Spotless	Brookfield	Spotless	Transfield	RD C&W	Ron Hunter	C&W (DBSMIC)	Simon Buckley
Base Services Support Centre (BSSC)	Transfield	Spotless	Brookfield	Spotless	Transfield	RD C&W	Ron Hunter	C&W (DBSMIC)	Simon Buckley
Commercial Ops Woomera (COW)	Transfield	N/A	N/A	N/A	N/A	RD C&W	Ron Hunter	C&W (DBSMIC)	Simon Buckley
Special Forces Training Facilities (SFTF)	Transfield	N/A	Brookfield	N/A	N/A	RD C&W	Ron Hunter	C&W (DBSMIC)	Simon Buckley
Training Areas and Range Management	Transfield	Spotless	Brookfield	Spotless	Transfield	RD C&W	Ron Hunter	DG BPESP (DOTAM)	Col David Graham
Transport	Transfield	Spotless	Brookfield	Spotless	Transfield	RD C&W	Ron Hunter	DS VT (DTAFS)	Bob Hogan
Airfield Ops	Transfield	Spotless	Brookfield	Spotless	Transfield	RD C&W	Ron Hunter	DS VT (DTAFS)	Bob Hogan
Estate Appraisal	Transfield	Spotless	Brookfield	Spotless	Transfield	RD C&W	Ron Hunter	ASES (DEPU)	Marcus Jeffery
Estate Upkeep	Transfield	Spotless	Brookfield	Spotless	Transfield	RD C&W	Ron Hunter	ASES (DEPU)	Marcus Jeffery
Laundry & Dry Cleaning	Transfield	Spotless	Brookfield	Spotless	Transfield	RD C&W	Ron Hunter	DS QLD (DGUS)	Craig Mills
Land Management	Transfield	Spotless	Brookfield	Spotless	Transfield	RD C&W	Ron Hunter	DS SNSW (DLMU)	Julie Groenendijk
Pest & Vermin	Transfield	Spotless	Brookfield	Spotless	Transfield	RD C&W	Ron Hunter	DS SNSW (DLMU)	Julie Groenendijk
Cleaning	Transfield	Spotless	Brookfield	Spotless	Transfield	RD C&W	Ron Hunter	DS SNSW (DLMU)	Julie Groenendijk
Housekeeping	Transfield	Spotless	Brookfield	Spotless	Transfield	RD C&W	Ron Hunter	DS SNSW (DLMU)	Julie Groenendijk
Base Reprographics	N/A	Spotless	N/A	Spotless	N/A	RD C&W	Ron Hunter	DS VT DLIS	Carl Fitchett
Sport & Recreation	Transfield	Spotless	Brookfield	Spotless	Transfield	RD C&W	Ron Hunter	DS QLD (DGUS)	Craig Mills
Access Control	Wilson	MSS Security	MSS Security	Wilson	Wilson	DG BPESP	CDRE Jaimie Hatcher	DG BPESP (DBSSP)	Dan Curtis
H&C	Transfield	Compass	Compass	Compass	Transfield	RD QLD/RD C&W	Gerald Griffin/Ron Hunter	DS QLD (DGUS)	Craig Mills
Waste	Veolia	Veolia	Veolia	Veolia	Veolia	RD SNSW	Julie Groenendijk	DS SNSW (DLMU)	Julie Groenendijk
Rescue & Fire Fighting	Transfield	Transfield	N/A	Transfield	Transfield	RD C&W	Ron Hunter	DS VT (DTAFS)	Bob Hogan
Aircraft Refuelling	Transfield	Transfield	N/A	Transfield	Transfield	RD C&W	Ron Hunter	ASES (DFRS)	Inger Carpenter [Acting]
POL	Transfield	Transfield	Transfield	Transfield	Transfield	RD C&W	Ron Hunter	ASES (DFRS)	Inger Carpenter [Acting]
Retail Stores	Transfield	Transfield	Transfield	Transfield	Transfield	RD C&W	Ron Hunter	ASES (DFRS)	Inger Carpenter [Acting]
National Program Service (NPS)	United Group	United Group	United Group	United Group	United Group	ASES	Mike Healy	ASES (DEWPO)	Kevin Fogarty
Project Delivery Service (PDS)	Augility and Aurecon	Augility and Aurecon	Augility and Aurecon	Augility and Aurecon	Augility and Aurecon	ASES	Mike Healy	ASES (DEWPO)	Kevin Fogarty
Directorate of Contract Governance	Contract Administrator - Coordinates B2B; Strat Review and DSO Input to BSCC meetings. Guidance on interpretation of T&Cs					DS NNSW	Dana Reddy	DS NNSW (DCG)	Dana Reddy
Contract Administration Support	Contract Support (CCPs; Contract notices; VFM assessment of CCPs; contract extensions; purchase orders; tracking price indexation; processing abatements; maintaining contract documents and price schedules)					DS NNSW	Dana Reddy	DS NNSW (DCG)	Dana Reddy

Annex I – CAMPUS Screenshot showing Objective courses

Campus - Windows Internet Explorer

File Edit View Favorites Tools Help x Convert Select

My Calendar My Account Help Log Out

 campus

My Campus

Home

Course Search

Search

Browse By Category

My Enrolments

My Curricula

My Completions

Order History

Evaluations & Surveys

Financial Delegations

Reports

Statistics

Search

Courses Offerings Curricula

Advanced Search


Search Objective Search

Courses

Title	Version	Course ID	Offerings	Actions
Advising Government and Ministers	1.0	00005368	11	Display Offerings
Army Objective Force (AOF)	1.0	00005628	1	Display Offerings
Objective Implementation Project Training for Senior Personnel	1.0	00006448	0	Display Offerings
Objective User Training	2.0	00007931	1	Display Offerings
Optimizing Your Work/Life Balance: Analyzing Your Life Balance	1.0	00002364	1	Display Offerings
Workgroup Coordinator	1.0	00005011	46	Display Offerings
Workplace Trainer	1.0	00005049	12	Display Offerings

Annex J – Objective User Account Access Request via ICT Service Portal (Post CAMPUS Training)

To have your Objective user account created, activated or updated, you must use the "Objective Access" item in the Service Request Catalogue - opposite.



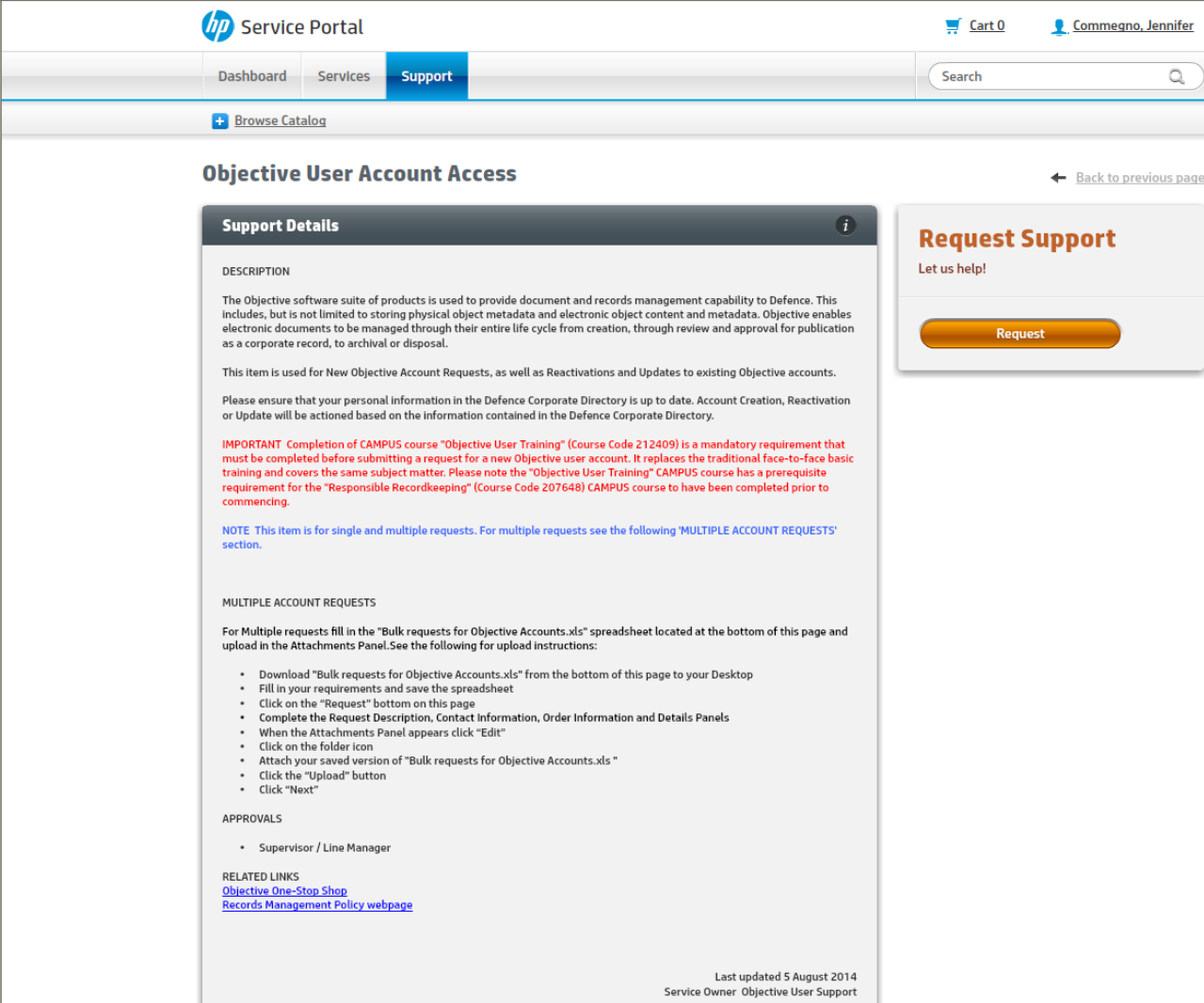
Click

Step 1 *(mouse-over for detail)*
Click the "**Submit**" button.

Step 2 *(mouse-over for detail)*
In the "**Description**" opposite, enter text as shown in the example above (mouse-over this Step 2 box to display example above).
Click Continue.

Step 3 *(mouse-over for detail)*
In the "**Details**" opposite, select the option you require then enter your **Directorate** and **Branch** details as **acronyms** (mouse-over this Step 3 box to display the example above).

All other details required for an Objective account will be sourced from the Defence Corporate Directory (DCD)
Please ensure your details in the DCD are up to date!



Objective User Account Access

Support Details

DESCRIPTION

The Objective software suite of products is used to provide document and records management capability to Defence. This includes, but is not limited to storing physical object metadata and electronic object content and metadata. Objective enables electronic documents to be managed through their entire life cycle from creation, through review and approval for publication as a corporate record, to archival or disposal.

This item is used for New Objective Account Requests, as well as Reactivations and Updates to existing Objective accounts.

Please ensure that your personal information in the Defence Corporate Directory is up to date. Account Creation, Reactivation or Update will be actioned based on the information contained in the Defence Corporate Directory.

IMPORTANT Completion of CAMPUS course "Objective User Training" (Course Code 212409) is a mandatory requirement that must be completed before submitting a request for a new Objective user account. It replaces the traditional face-to-face basic training and covers the same subject matter. Please note the "Objective User Training" CAMPUS course has a prerequisite requirement for the "Responsible Recordkeeping" (Course Code 207648) CAMPUS course to have been completed prior to commencing.

NOTE This item is for single and multiple requests. For multiple requests see the following 'MULTIPLE ACCOUNT REQUESTS' section.

MULTIPLE ACCOUNT REQUESTS

For Multiple requests fill in the "Bulk requests for Objective Accounts.xls" spreadsheet located at the bottom of this page and upload in the Attachments Panel. See the following for upload instructions:

- Download "Bulk requests for Objective Accounts.xls" from the bottom of this page to your Desktop
- Fill in your requirements and save the spreadsheet
- Click on the "Request" button on this page
- Complete the Request Description, Contact Information and Details Panels
- When the Attachments Panel appears click "Edit"
- Click on the folder icon
- Attach your saved version of "Bulk requests for Objective Accounts.xls"
- Click the "Upload" button
- Click "Next"

APPROVALS

- Supervisor / Line Manager

RELATED LINKS

[Objective One-Stop Shop](#)
[Records Management Policy webpage](#)

Last updated 5 August 2014
Service Owner Objective User Support

Annex K – Objective Contractor Access Request Form to Estate Management Folders

Objective

Contractor Access Request

Date	<input type="text" value="27/01/15"/>	Reference:	<input type="text"/>
------	---------------------------------------	------------	----------------------

Contractor Details Completed by Contractor

DRN User Name :	<input type="text"/>	Region:	<input type="text"/>
DRN Email:	<input type="text"/>	Security:	<input type="text"/>
Contractor Company:	<input type="text"/>		
Sub-Contractor Company:	<input type="text"/>		
Reason for Access/Change:	<input type="text"/>		

Defence Sponsor Details Completed by DSRG Staff

Sponsor Name:	<input type="text"/>
Sponsor Email:	<input type="text"/>
Position:	<input type="text"/>
Directorate / Business Unit:	<input type="text"/>

Access Requirements Completed by DSRG Staff

Region/Directorate Folder:	<input type="text"/>	Objective Folder/File ID:	<input type="text"/>
Action Required:	<input type="radio"/> Add <input type="radio"/> Remove <input type="radio"/> Move <input type="radio"/> Change Access		
Change to access for which Folders/Files? (List)	<input type="text"/>		
Level of Access Required:	<input type="checkbox"/> See Only <input type="checkbox"/> Open <input type="checkbox"/> Create <input type="checkbox"/> Edit		
Access From:	<input type="text"/>	To:	<input type="text"/>
<small>Note: Sponsor to advise WGC for removal earlier than these dates.</small>			

Sponsor Endorsement

Signature Field	<input type="text"/>	Comments	<input type="text"/>
-----------------	----------------------	----------	----------------------

Contractor Objective Coordinator Endorsement Contractor Manager / Primary Contractor

Signature Field	<input type="text"/>	Comments	<input type="text"/>
-----------------	----------------------	----------	----------------------

Work Group Coordinator Endorsement

Contractor User Group Name:	<input type="text"/>		
Signature Field	<input type="text"/>	Access Granted:	<input type="checkbox"/>
		Sponsor Advised:	<input type="checkbox"/>
		Review Date:	<input type="text"/>

Filing Instruction - Naming Convention: [Review Year/Month - Name of Contractor Person - WGC Initials]

Annex L – Minimum Scanning Specifications (Extract from RECMAN)

Table 4A.1: Records types and standards Record Type	Standard		Quality Check
<p>For clean, high contrast documents with text or graphics, for which colour is either not present or not essential, and for any images that are line art, Defence must produce images conforming to these specifications or higher. Generally this specification for documents may be used unless any of the following conditions apply:</p> <p>The document contains colour information that must be retained to preserve the meaning;</p> <p>The document has a low contrast (eg faded text, browning paper, or coloured paper); or</p> <p>The document includes photographs, is a photograph or a negative.</p> <p>Please Note: documents with coloured letterheads, wet signatures (unless they have</p>	Format	JPEG 2000, PDF/A, TIFF	Testing of the images to ensure that the minimum requirements listed in these technical specifications have been met.
	Multi page format	PDF/A	
	Resolution	300 dpi	
	Scanning ratio	100%	
	Type of image	greyscale	
	Bit-depth	8 bit	
	Compression	lossy	
	Searchability	OCR Recommended	

Annex M – Document Descriptors, File Placement, Key Stakeholders and Estimated Document Size

Document Descriptors	Applicable Acronym	Where Object Should be Placed in Objective Estate Management Folder(s)	Who should have visibility of this type of document if not in IBIS?	Expected Size of File (S, M, L, XL)*
Airfield Ground Lighting (AGL) Dispensation	AGLD	EM: Estate object		S
Asbestos Hazard Identification Report	AHIR	EM: Estate object	EFS, BSM, Projects, Contractor	S
Asbestos Survey Report	ASR	EM: Estate object		L
Audit Report	AUDR	EM: Estate object Other: As Advised	As determined by PSM/CA	L
Bank Guarantee	BNKG	Dept of Treasury	DCG/CAS/Finance	S
Building Code of Australia Alternative Solution	BCAS	EM: Estate object		M
Bushfire Report	BFR	EM: Estate object		L
Business Case	BUSC	EM: Estate object Relevant Directorate	As Determined	S
CAD File	CAD	EM: Estate object		L
Certificate Of Occupancy	COO	EM: Estate object	EFS (Property), BSM, Projects, Contractor	S
Certificate of Title	COT	EM: Estate object		S
Commissioning and Handover Plan	CHP	Relevant Directorate	As Determined	M
Commissioning Report	COMR	Relevant Directorate	As Determined	M
Compliance Certificate / Certificate of Compliance	COC	EM: Estate object		S
Concept Design Report	CDR	EM: Estate object		L
Contract	CONT	DCG Relevant Directorate	Restricted - Relevant Directorate	M
Contract Amendment Proposal	CAP	EM: CCP Folder	Contractor, PSM, DPCB and CA	S
Contract Change Proposal	CCP	EM: Estate object	EFS, BSM, Projects, Contractor	M
Corporate Services Infrastructure Requirement	CSIR	EM: Estate object	EFS, BSM, Projects, Contractor	M

Defence Dispensation	DISP	Relevant Directorate	As Determined	S
Design Recommendations	DESR	Relevant Directorate	As Determined	L
Design Report	DREP	Relevant Directorate	Projects, Contractor, EFS	L
Email	EML	As Determined	As Determined	S
Engineering Report	ENGR	EM: Estate object		L
Estate Investment Requirement	EIR	EM: Estate object	EFS, BSM, Projects, Contractor	M
Fire Safety Survey Report	FSS	EM: Estate object		L
Functional Design Brief	FDB	Relevant Directorate	As Determined	L
Geospatial Shape File	GSF	EM: Estate object		L
Governance	GOVR	Restricted	CAS/DCG/CAs	S
Green Star Rating	GSR	EM: Estate object		M
Hazard Area Verification Dossier	HAVD	EM: Estate object		M
Heritage Report	HERR	EM: Estate object		L
Image	IMG	EM: Estate object NSIMS		L
Impact Assessment	IMPA	EM: Estate object		M
Incident Report	INCR	EM: Estate object Sentinal	WHS, Contractor, PSM, CA, BSM, EFS, RD	S
Inspection Report	INSP	EM: Estate object		M
Invoice	INV	Relevant Directorate	CAS/DCG	S
Lease	LEAS	EM: Estate object	DRH/PPP, EFS (Property)	M
Legal Report	LEGR	Relevant Directorate	DPCB/DCG	M
Legal Title	LEGT	Relevant Directorate	As Determined	S
Letter of Acceptance	LOA	Relevant Directorate	As Determined	S
Management Plan	MANP	EM: Contractor Deposit Box	PSM, CA, DCG, Contractor	M
Manufacturers Specification	MANS	EM: Estate object		M
Map	MAP	NSIMS	EFS, Projects, BSM,	L
Manual of Fire Protection Engineering (MFPE) Dispensation	MFPED	EM: Estate object		S
NABERS (ie Building Energy	NABER	EM: Estate object		S

Use) Rating				
Net Personnel Operating Costs (NPOC) Report	NPOC	Relevant Directorate	NPOC is being phased out	S
Operation and Maint Manual	OMM	EM: Estate object Relevant Property File		M
Performance Report	PERF	EM: Contractor Deposit Box	PSM, CA, Contractor, DCG, BSM	S
Procurement Plan	PROC	EM: Contractor Deposit Box	DPCB, PSM, CA, BSM	S
Project Brief	PROB	EM: Estate object Relevant Directorate(s)	As Determined	M
Project Control	PROC	Relevant Directorate	As Determined	S
Project Management Plan	PMP	Relevant Directorate	As Determined	M
Project Proposal	PROP	Relevant Directorate	As Determined	S
Project Schedule	PROS	Relevant Directorate	As Determined	S
Project Scope Recommendation	PSR	Relevant Directorate	As Determined	S
Project Specification	SPEC	Relevant Directorate	As Determined	S
Project Variation	PROV	Relevant Directorate	As Determined	S
Registration	REGI	Relevant Directorate	As Determined	S
Request for Tender	RFT	Relevant Directorate	As Determined	M
Risk Assessment	RASS	EM: Estate object Relevant Directorate	As Determined	S
Scope of Works	SOW	EM: Estate object		M
Service Delivery Plan	SDP	EM: Estate object		S
Site Selection Report	SSR	EM: Estate object		M
Stakeholder Management Plan	SMP	Relevant Directorate	As Determined	S
Submitted Tenders	SUBT	Relevant Directorate	As Determined	M
Tender Evaluation Plan	TEP	Relevant Directorate	As Determined	S
Warranty	WARR	EM: Estate object		S
			Key S M	Less than 10MB Between 10 and 100 MB

L Between 100 MB to 1GB
XL Over 1 GB
EM Estate Management folder grouping

Subject area specific documentation

Document Descriptors	Applicable Acronym	Where Object Should be Placed in Objective Estate Management Folder(s)	Who should have visibility of this type of document if not in Estate object?	Expected Size of File (S, M, L, XL)*
Defence Fuel Installation related material	DFI + Applicable Acronym	Relevant Property File	PSM Fuel and Retail Stores, PSM Estate Planning & Upkeep	S, M, L, XL

(Electronic copy embedded – double click to open)

43 of 46

Acronyms

In this document, all references to an acronym in the singular also refers to the plural, and vice versa.

ADF	<i>Australian Defence Force</i>
ASES	<i>Assistant Secretary Estate Owners</i>
BAU	<i>Business-As-Usual</i>
BS	<i>Base Services</i>
BPO	<i>Business Process Owners</i>
CA	<i>ESD Contract Authorities</i>
CIOG	<i>Chief Information Officer Group</i>
DBO	<i>Data Business Owner</i>
DCPB	<i>Defence Contracting and Procurement Branch</i>
DDIG	<i>Director Data and Information Governance</i>
DEIS	<i>Defence Estate Information Systems. Means each of the Commonwealth's estate information management systems.</i>
DEMS	<i>Defence Estate Maintenance System</i>
DEQMS	<i>Defence Estate Quality Management System</i>
DFTP	<i>Defence Functional Transfer Plan</i>
DGPESP	<i>Director General Base Planning, Engagement and Service Performance</i>
DISP	<i>Defence Industry Security Program</i>
DPCB	<i>Defence Procurement Contracting Branch</i>
DPEP	<i>Director Partner Engagement and Performance</i>
DPP	<i>Director Planning and Programming</i>
DRN	<i>Defence Restricted Network</i>
ESD	<i>Estate Services Division Division</i>
E&IG	<i>Estate and Infrastructure Group (previously DSRG)</i>

EMOS	<i>Estate Maintenance and Operation Services</i>
GEMS	<i>Garrison and Estate Management System</i>
HDSO	<i>Head Estate Services Division</i>
Estate object	<i>Interim Business Intelligence System</i>
ID	<i>Infrastructure Division</i>
MSP	<i>Miscellaneous Service Package</i>
Objective	<i>Objective is the Defence electronic file and records management system.</i>
PSM	<i>ESD Product Service Manager</i>
RD	<i>Regional Director</i>
RMF	<i>Risk Management Framework</i>
SADFO	<i>Senior ADF Officer</i>
Service Line	<i>Is the individual set of service requirements which reflects an individual Statement of Work, its supporting information and data that describes the requirements for a specific service or product</i>